October 24, 2024

From Horsepower to Data Power: The New Era of Driving with an AI Engine and Privacy Bumpers

David Cox
Volkswagen

Jim Gregoire
Rivian

Alma Murray
Lucid Motors

Laura Hamady, Moderator
Troutman Pepper

Privacy+ Security Forum

Speakers

David Cox

Assistant General Counsel - Privacy, Data Governance, & E-Discovery
Volkswagen

Jim Gregoire

Senior Director, Privacy
Rivian

Alma Murray

Assistant General Counsel, Global Privacy and Data Security Programs
Lucid Motors

Laura Hamady

Privacy & Cyber Counsel
Troutman Pepper

AI in Vehicles – Background, Benefits and Context

Privacy+ Security Forum

SAE AUTOMATION LEVELS

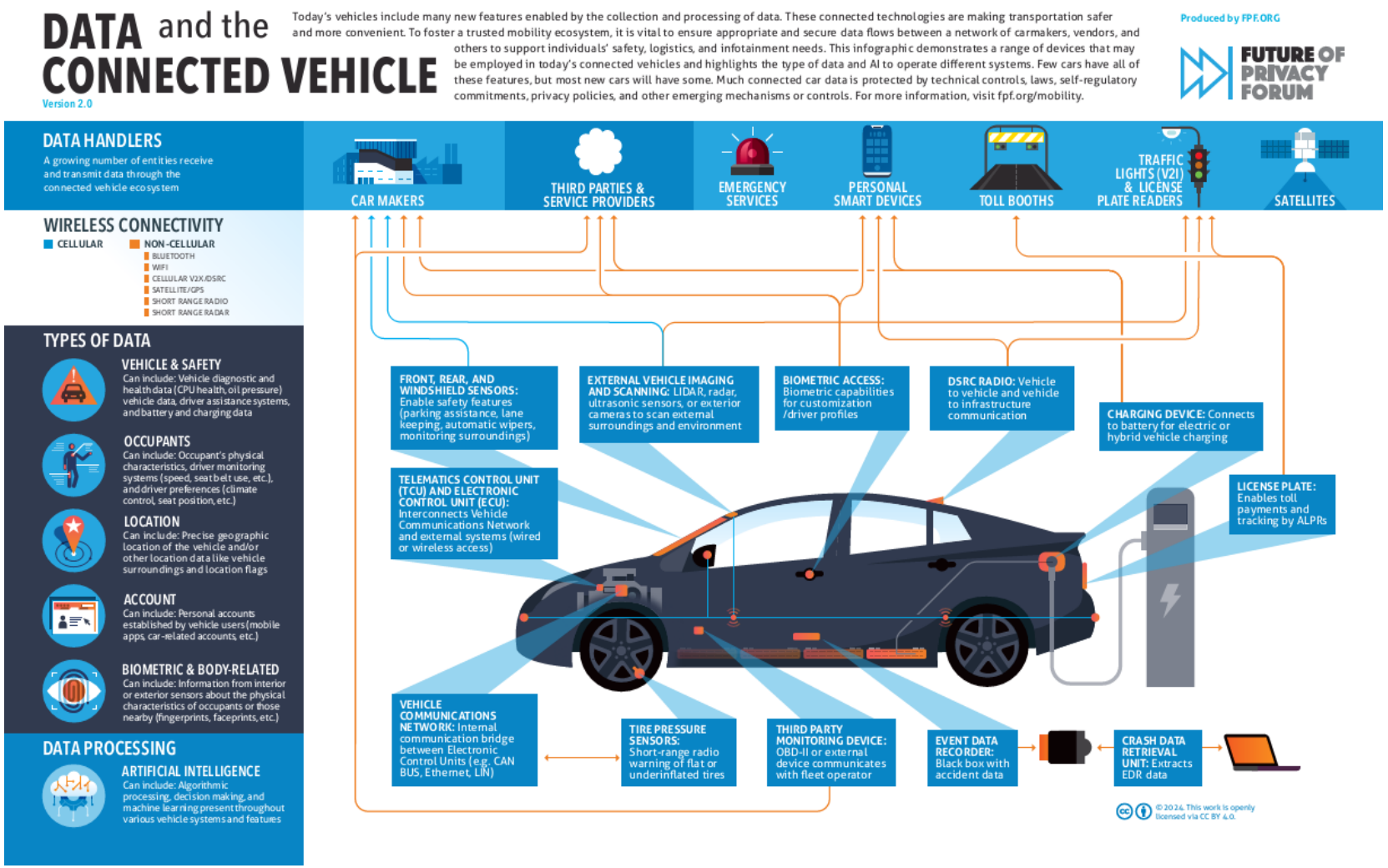
Full Automation

0	1	2	3	4	5
No Automation	Driver Assistance	Partial Automation	Conditional Automation	High Automation	Full Automation
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Source: Automated Driving System 2.0 - Voluntary Guidance from USDOT NHSTA.pdf

Data and the Connected Car

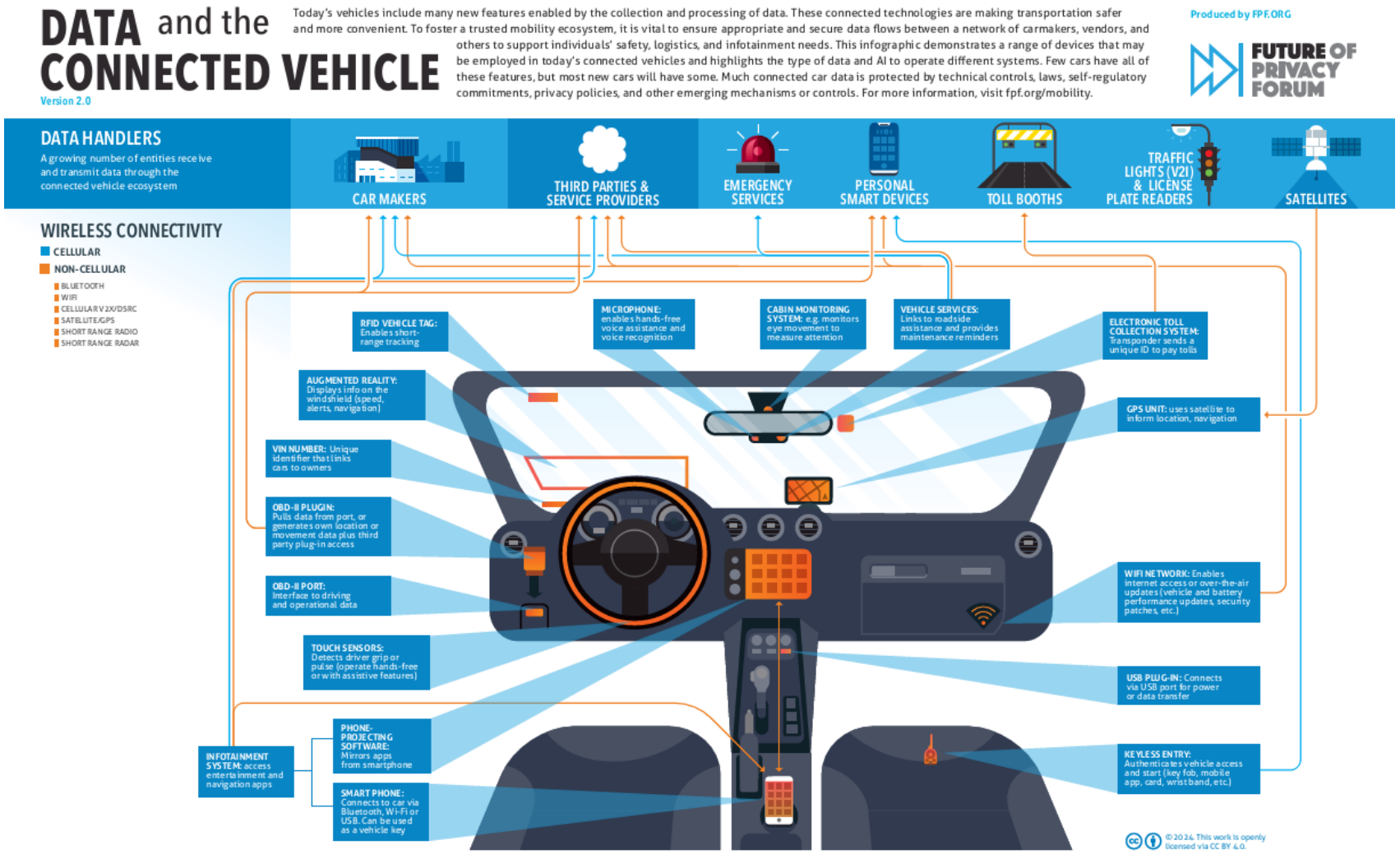
Privacy+ Security Forum



Source: [FPF_connected_vehicl_i03]

Data and the Connected Car

Privacy+ Security Forum



Source: FPF_connected_vehicl_i03

Use Cases of AI in the Automotive Industry

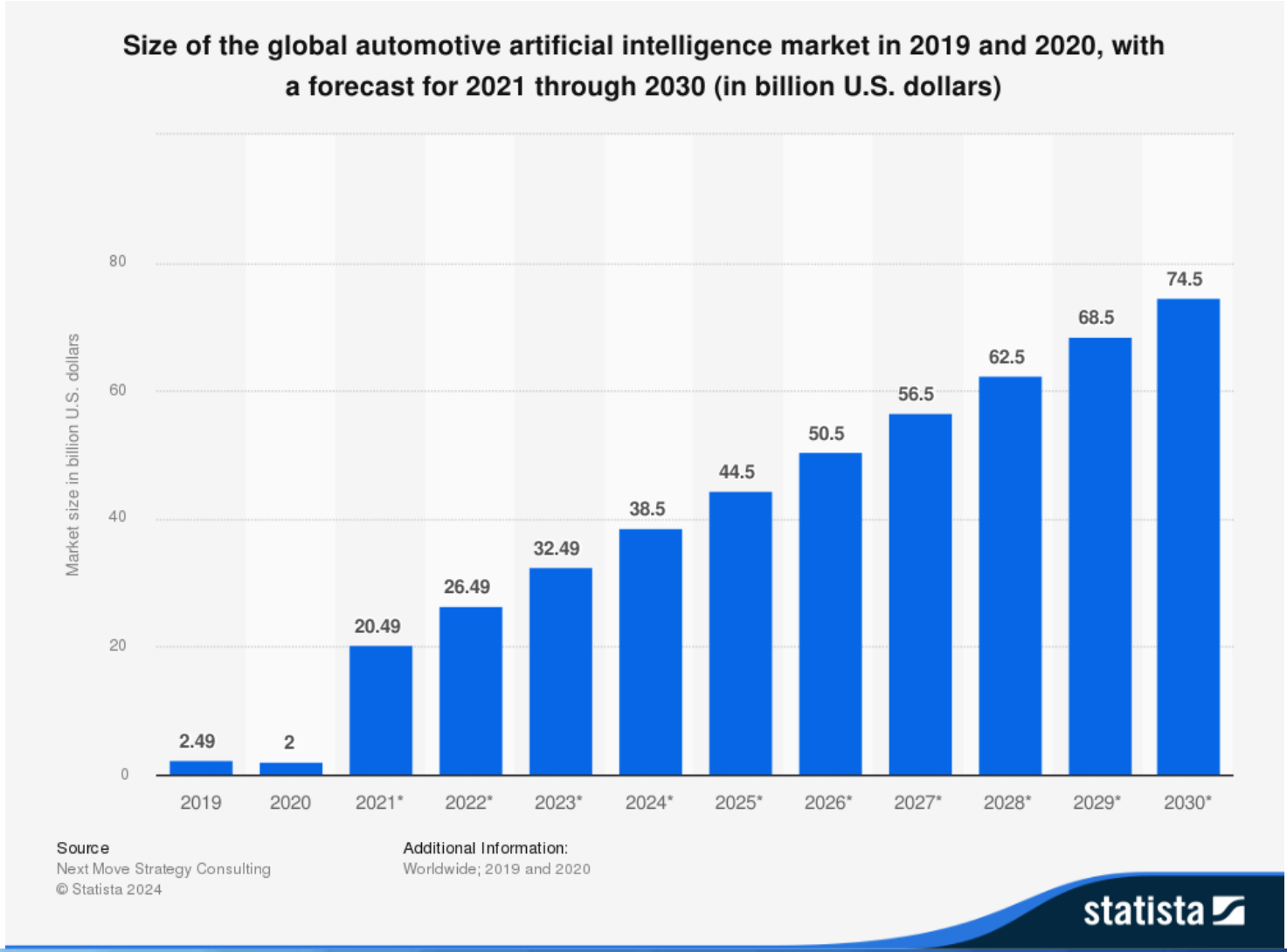
Privacy+ Security Forum

- Driver Assistance
- Autonomous Vehicles
- Driver Monitoring
- AI in Manufacturing
- Personal Assistance
- Passenger Experience
- Supply Chain Management
- Automotive Insurance
- Quality Control
- Connected Cars
- AI in Designing

Source: https://appinventiv.com/

Forecast for Growth: Global Auto + AI Market in 2030

Privacy+ Security Forum



Source: Automotive AI global market size | Statista

Vehicle Data Excerpts

Privacy+ Security Forum

PROPERTY_NAME	DESCRIPTION, PURPOSE, AND USE
EMS_charger_evse_type	Indicates the type of EVSE connected to the charger to ensure compatibility and optimal charging performance
EMS_charger_exit_status	Indicates the exit status of the charger to ensure proper operation and detect any faults or errors
EMS_charger_mode_state	Indicates the current mode state of the charger to ensure proper operation and detect any changes in charging modes
charger_type_detected	To identify the type of charger connected. Properly configuring charging parameters
schedule_status	To indicate the status of the charging schedule
EMS_charger_sm_timeout_status	To determine if the charger state machine has timed out
voltage	Used to monitor the actual voltage of the main battery pack
voltage_max	Used to set the maximum voltage limit for the main battery pack
current	Used to monitor the actual current of the main battery pack
current_feedback	To monitor the current flowing in the battery to analyze battery usage patterns and detect any abnormalities
trigger_cb0	Trigger for circuit breaker reset 0. Initiating a circuit breaker reset.
trigger_cb1	Trigger for circuit breaker reset 1. Initiating a circuit breaker reset.
service_mode	Service mode of the Electronic Park Brake (EPB). To enter service mode for maintenance or repairs.
warning_lamp	Warning lamp of the Electronic Park Brake (EPB) to indicate a warning or fault in the EPB system
message_display_request	To display a specific message related to the EPB
tire_FL_pressure_status	Tire pressure status for front left tire
tire_FR_pressure_status	Tire pressure status for front right tire
tire_FL_pressure_status_valid	Validation status for front left tire pressure
tire_FR_pressure_status_valid	Validation status for front right tire pressure

Vehicle Data Example

Privacy+ Security Forum

Spreadsheet of speed readings

Speed
63 mph
37 mph
42 mph
29 mph
Etc.

+ pseudoID

Car ID
1541230
1840368
1592143
1250308
Etc.

+ VIN

VIN
7PDDGEBLXXN123453
7PDDGEBLXXN123454
7PDDGEBLXXN123455
7PDDGEBLXXN123456
Etc.

+ Date and Time

Date	Time
10/22/24	2:02 pm
10/22/24	5:33 pm
10/22/24	6:25 am
10/22/24	11:13 pm
Etc.	

+ Known Driver

Driver
Jim Gregoire
Alma Murray
David Cox
Laura Hamady
Etc.

Less personal

More personal

Compliance Considerations and Challenges in the Modern Automotive Space

Privacy+ Security Forum

Growth of Automotive Data Types Boosted by AI

Privacy+ Security Forum

- **Autonomous driving:** Data on all levels, from L1 to L5, including that collected from the multiple sensors installed on vehicles.
- **Infrastructure:** Remote monitoring, OTA updates, and data used for remote control by control centers, V2X, and traffic patterns.
- **Infotainment:** Information on how customers are using applications, such as voice control, gesture, maps, and parking.
- **Connected information:** Information on payment to third-party parking apps, accident information, data from dashboard cameras, handheld devices, mobile applications, and driver behavior monitoring.
- **Vehicle health:** Repair and maintenance records, insurance underwriting, fuel consumption, telematics.

Source: Increased Automotive Data Use Raises Privacy, Security Concerns (semiengineering.com)

Common Types of Automotive Data

Privacy+ Security Forum

Legacy Data Types

Event Data Recorders – EDRs **have been integrated into cars for decades and are in around 90% of vehicles** and must meet federal requirements. ECRs record technical information about a vehicle's operation in the seconds before and after a crash. Data types include **speed, accelerator and brake position, seat belt usage, and whether the airbags deployed.** EDRs are intended to provide crucial information to crash investigators and others. **Accessing EDR information requires physical access to the vehicle as well as a specific EDR reader tool, in addition to meeting any consent requirements for a given state** and additional laws governing ownership of EDR data vary state by state.

On-Board Diagnostic Information – All vehicles manufactured after 1996 are legally required to have an On-Board Diagnostic port, or "OBD-II."

OBD-II data may include driver behavioral information (how fast you drive, how aggressively you apply the brakes, etc.) as well as geolocation data (where you are, where you have traveled, and your speed)

OBD-II data can be retrieved by physically inserting a compatible device into the port and is intended to help service technicians measure emissions, diagnose performance issues, or repair vehicles. **Owners may also choose to plug in a third-party device (or "dongle") into the OBD-II port in some vehicles to collect or share information about their vehicle with third parties** of (for example, with an insurance company to gain safe driving discounts).

Source: Increased Automotive Data Use Raises Privacy, Security Concerns (semiengineering.com)

Common Types of Automotive Data

Privacy+ Security Forum

New(er) Data Types

Location Information – **Collected by navigation and related systems for routing purposes.**

External Information – Data collected by cameras and external sensors that are used to gather information about a vehicle's immediate surroundings such as **road or weather conditions, lane markings and obstacles, surrounding traffic**, etc.

Key safety technologies like blind spot detection, lane-departure warnings, assisted braking, and rear-parking detection rely on this external environmental information.

In-Cabin Information – Data collected by microphones, cameras, and other devices in the vehicle can be used to collect information about vehicle interior and its occupants. These sensors **can help drivers use safety features** for example, to communicate with emergency services or to utilize features such as hand-free telephone use.

Source: Increased Automotive Data Use Raises Privacy, Security Concerns (semiengineering.com)

Common Types of Automotive Data

Privacy+ Security Forum

New(er) Data Types

User Recognition – Some vehicles use technologies that recognize users by **physical characteristics such as a fingerprint or face or other data** (i.e. collect physical, or diametric, or biometric information) can also be used to grant access to automotive features or customize settings. These technologies can also track eye movement to detect attentiveness to help prevent unsafe driving behaviors.

Apps –Some vehicles may include interfaces with third-party systems like Apple CarPlay, Android Auto, etc. These generally add functionality to the driving experience for the driver but can, in some cases, expose data from the car to the app provider.

Other – Vehicle manufacturers and their technology partners are constantly updating and improving vehicles for convenience and safety

Source: Increased Automotive Data Use Raises Privacy, Security Concerns (semiengineering.com)

Getting Practical: How to Drive Compliance in the Business Setting

Privacy+ Security Forum

INVEST IN GOVERNANCE + MAKE IT REAL

Privacy+ Security Forum

1. **Invest in Governance – Establish formal AI governance program to oversee AI development and deployment**
    - Overarching AI policy, initiative tracker
    - AI Steering Committee
    - Dedicated AI resources (can't do this part-time)
    - Implement AI checks in other key risk management processes (e.g., privacy review, TPRM, procurement)
2. **Make it Real – Implement a multi-pronged approach to notice and consent to maximize visibility and utility for customers**
    - Initial notice upon change (e.g., OTA Release Notes)
    - Updated Data Privacy Notice
    - Just-in-time Notices in the vehicle upon use (e.g., pop-ups or icons)
    - Choice regarding use of the AI feature and whether data is used for training

STREAMLINE COMPLIANCE + DATA, DATA, DATA!

Privacy+ Security Forum

3. **Streamline compliance into existing business process – Integrate AI risk assessment in your existing privacy review/PbD processes**
   - Questions in your high-level/initial privacy assessment
   - Deeper-dive AI assessment for your PIAs
   - Longer-term, consider developing a quantitative risk scoring rubric for AI-related initiatives
4. **Data, data, data! Establish a robust data governance program that requires accountability of data and system owners to limit what data is available to AI models**
   - Data definitions, classifications up front (to flow down to other systems and govern uses)
   - Access controls matched to data sensitivity and use
   - Periodic reporting and compliance testing

GET OUT THERE AND STAY IN THE MIX + DOG FOOD!

Privacy+ Security Forum

5. **Get out there and stay in the mix. Collaborate with customers, peers, regulators, industry bodies to develop AI standards for your technology**
   - Meet regularly with your Public Policy team to track trends and proposed legislation, meet with legislators
   - Provide feedback during public comment periods
   - Conduct customer focus groups to understand their needs and concerns
   - Speak regularly with peers at industry events and calls
6. **Dog food! Trust but verify – use your products, define review and testing criteria for AI models and make certain they work n practice, not just on paper.**
   - AI is still so new. Lots of promises will be made, but many may not be met.
   - Define testing criteria/thresholds based on AI risk (e.g., type or volume of data, use case)
   - Ensure sufficient technical expertise to properly review the model
   - Check that use is consistent with contractual provisions

Questions & Contacts

Privacy+ Security Forum

David Cox

Assistant General Counsel - Privacy, Data Governance, & E-Discovery
Volkswagen

Jim Gregoire

Senior Director, Privacy
Rivian

Alma Murray

Assistant General Counsel, Global Privacy and Data Security Programs
Lucid Motors

Laura Hamady

Privacy & Cyber Counsel
Troutman Pepper